

WARRANT FOR ARREST

United States District Court		DISTRICT SOUTHERN DISTRICT OF NEW YORK	
UNITED STATES OF AMERICA v. ALEX HATALA, a/k/a "kool+kake"		DOCKET NO. <div style="font-size: 1.5em; font-weight: bold;">1211 MAG 1669</div>	MAGISTRATE'S CASE NO.
WARRANT ISSUED ON THE BASIS OF: <input type="checkbox"/> Order of Court <input type="checkbox"/> Indictment <input type="checkbox"/> Information <input checked="" type="checkbox"/> Complaint		NAME AND ADDRESS OF INDIVIDUAL TO BE ARRESTED ALEX HATALA, a/k/a "kool+kake" 221 Five Pounds Road, St. Simons Island, GA 31522	
TO: UNITED STATES MARSHAL OR ANY OTHER AUTHORIZED OFFICER		DISTRICT OF ARREST	
CITY			
YOU ARE HEREBY COMMANDED to arrest the above-named person and bring that person before the United States District Court to answer to the charge(s) listed below.			
DESCRIPTION OF CHARGES			
Fraud in Connection with Identification Information			
IN VIOLATION OF	UNITED STATES CODE TITLE 18	SECTION 1028(a)(7)	
BAIL	OTHER CONDITIONS OF RELEASE		
ORDERED BY	SIGNATURE (FEDERAL JUDGE/U.S. MAGISTRATE)		DATE ORDERED <div style="font-size: 1.2em; font-weight: bold;">JUN 22 2012</div>
CLERK OF COURT	(BY) DEPUTY CLERK		DATE ISSUED
ANDREW J. PECK UNITED STATES MAGISTRATE JUDGE RETURN SOUTHERN DISTRICT OF NEW YORK			
This warrant was received and executed with the arrest of the above-named person.			
DATE RECEIVED	NAME AND TITLE OF ARRESTING OFFICER	SIGNATURE OF ARRESTING OFFICER	
DATE EXECUTED			

Note: The arresting officer is directed to serve the attached copy of the charge on the defendant at the time this warrant is executed.

Approved: _____

SERRIN TURNER

Assistant United States Attorney

Before: HONORABLE ANDREW J. PECK
United States Magistrate Judge
Southern District of New York

12
MAG

- - - - - X
:
UNITED STATES OF AMERICA : SEALED COMPLAINT
:
- v. - : Violation of
: 18 U.S.C. § 1028(a)(7)
ALEX HATALA, :
a/k/a "kool+kake," : COUNTY OF OFFENSE:
: New York
Defendant. :
:
- - - - - X

SOUTHERN DISTRICT OF NEW YORK, ss.:

Christopher J. Cope, being duly sworn, deposes and says that he is a Special Agent with the Federal Bureau of Investigation ("FBI") and charges as follows:

COUNT ONE

(Fraud in Connection with Identification Information)

1. From in or about December 2010, up to and including in or about July 2011, in the Southern District of New York and elsewhere, ALEX HATALA, a/k/a "kool+kake," the defendant, knowingly transferred, possessed, and used, without lawful authority, a means of identification of another person with the intent to commit, and to aid and abet, and in connection with, unlawful activity that constitutes a violation of Federal law, and that constitutes a felony under applicable State and local law, to wit, HATALA possessed stolen credit card information and stolen login information for online accounts at PayPal and other websites, and distributed such information to others who sought to use the information to facilitate fraudulent credit card transactions.

(Title 18, United States Code, Section 1028(a)(7).)

The bases for my knowledge and for the foregoing charge are, in part, as follows:

2. I have been personally involved in the investigation of this matter. This affidavit is based upon my investigation, my conversations with other law enforcement agents, and my examination of reports and records. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

3. I have been a Special Agent with the FBI for approximately three years. For the past two years, I have been assigned to the computer intrusion squad in the FBI's New York Field Office. I have received training regarding computer technology, computer fraud, and white collar crimes.

Background on the UC Site

4. Based on my training and experience, I have learned the following:

a. Carding: "Carding" refers to various criminal activities associated with stealing personal identification information and financial information belonging to other individuals - including the account information associated with credit cards, bank cards, debit cards, or other access devices - and using that information to obtain money, goods, or services without the victims' authorization or consent. For example, a criminal might gain unauthorized access to (or "hack") a database maintained on a computer server and steal credit card numbers and other personal information stored in that database. The criminal can then use the stolen information to, among other things: (1) buy goods or services online; (2) manufacture counterfeit credit cards by encoding them with the stolen account information; (3) manufacture false identification documents (which can be used in turn to facilitate fraudulent purchases); or (4) sell the stolen information to others who intend to use it for criminal purposes. "Carding" refers to the foregoing criminal activity generally and encompasses a variety of federal offenses, including, but not limited to, identification document fraud, aggravated identity theft, access device fraud, computer hacking, wire fraud, and bank fraud.

b. Carding Forums: "Carding forums" are websites used by criminals engaged in carding ("carders") to facilitate their criminal activity. Carders use carding forums to, among other things: (1) exchange information related to carding, such as information concerning hacking methods or computer-security vulnerabilities that could be used to obtain personal identification information; and (2) buy and sell goods and services related to carding, for example, stolen credit card or debit card account numbers, hardware for creating counterfeit credit cards or debit cards, or goods bought with compromised credit card and debit card accounts. Carding forums often permit users to post public messages (postings that can be viewed by all users of the site), sometimes referred to as "threads." For example, a user who has stolen credit card numbers may post a public "thread" offering to sell the numbers. Carding forums also often permit users to communicate one-to-one through so-called "private messages." Because carding forums are, in essence, marketplaces for illegal activities, access is typically restricted to avoid law enforcement surveillance. Typically, a prospective user seeking to join a carding forum can only do so if other, already established users "vouch" for the prospective user, or if the prospective user pays a sum of money to the operators of the carding forum. User accounts are typically identified by a username and access is restricted by password. Users of carding forums typically identify themselves on such forums using aliases or online nicknames ("nics").

5. Based on my participation in the investigation of this matter, I know the following:

a. In or about June 2010, the FBI established an undercover carding forum (the "UC Site"), enabling users to discuss various topics related to carding and to communicate offers to buy, sell, and exchange goods and services related to carding, among other things.

b. The FBI established the UC Site as an online meeting place where the FBI could locate cybercriminals, investigate and identify them, and disrupt their activities.¹ The UC Site was configured to allow the FBI to monitor and to record the discussion threads posted to the site, as well as private messages sent through the site between registered users.

¹ The registration process for the UC Site required users to agree to terms and conditions, including that their activities on the UC Site were subject to monitoring for any purpose.

The UC Site also allowed the FBI to record the Internet protocol ("IP") addresses of users' computers when they accessed the site.²

c. Access to the UC Site was limited to registered members and required a username and password to gain entry. Various membership requirements were imposed from time to time to restrict site membership to individuals with established knowledge of carding techniques or interest in criminal activity. For example, at times new users were prevented from joining the site unless they were recommended by two existing users who had registered with the site, or unless they paid a registration fee.

d. New users registering with the UC Site were required to provide a valid e-mail address as part of the registration process. An e-mail message was sent to that email address containing registration instructions. In order to complete the registration process, the new user was required to open the e-mail, click on a link in it, and then enter an activation code specified in the e-mail message. The e-mail addresses entered by registered members of the site were collected by the FBI.

e. In the course of the undercover operation, the FBI contacted multiple affected institutions and/or individuals to advise them of discovered breaches in order to enable them to take appropriate responsive and protective measures. Based on information obtained through the site, the FBI estimates that it helped financial institutions prevent many millions of dollars in losses from credit card fraud and other criminal activity, and has alerted specific individuals regarding breaches of their personal email or other accounts.

f. At all times relevant to this Complaint, the server for the UC Site, through which all public and private messages on the UC Site were transmitted, was located in New York, New York.

² Every computer on the Internet is identified by a unique number called an Internet protocol ("IP") address, which is used to route information properly between computers.

Possession and Distribution of Stolen
Credit Card and Login Information by "kool+kake"

6. As set forth below, ALEX HATALA, a/k/a "kool+kake," the defendant, was a user of the UC Site who possessed stolen credit card information and stolen login information for online accounts at PayPal and other websites, and distributed such information to others who sought to use the information to facilitate fraudulent credit card transactions.³

7. On or about December 16, 2010, an individual registered on the UC Site with the username "kool+kake."⁴

8. On or about December 19, 2010, "kool+kake" started a discussion thread titled "Location-Specific World Wide CVV's."⁵ From reviewing this posting, I know the following:

a. In the posting, "kool+kake" advertised that he had "CVV's" available for sale. Based on my training and experience, I know that the term "CVV" is used by carders to refer to credit card data that includes, among other information, the name, address, and zip code of the card holder, along with the card number, expiration date, and security code printed on the card.

b. "kool+kake" elaborated in the posting: "I will be selling location-specific cvv's- meaning you supply me with the city, state/province, and I will provide you with the live cvv(s). i'm not a wizard and don't have access to every single town, city in the world, but I can have quite a few in many locations." Based on my training and experience, I understand "kool+kake" to have meant by this remark that he could sell stolen credit card data based on the location of the address on the credit card account. Thus, a carder wanting to purchase

³ The FBI has taken steps to alert the affected credit card companies and websites of the compromised accounts to the extent they have been identified through the investigation.

⁴ Based on my familiarity with Internet slang, the intended pronunciation of this username is "cool and cocky."

⁵ Unless otherwise noted, all postings and private messages referred to herein were posted or sent on the UC Site and were retained as part of the operation of the UC Site. Quotations from such messages and any other electronic communications are reproduced substantially as they appear in the original text; errors in spelling and punctuation have not been corrected.

goods in a particular area of the country could buy a stolen credit card account from "kool+kake" based in that same area. In this way, the carder could avoid fraud alerts that otherwise might be triggered by the use of a credit card account outside its normal area of usage.

c. "kool+kake" stated that the card data he was selling would come in the following format: "cvv / exp yr / exp mo / ccn / country / zip / province / city/area / address / name / email."

d. "kool+kake" explained his method of acquiring the credit card accounts he had for sale as follows: "I did not buy these, I don't resell, I get these fresh and daily from DBs [databases] around the world." Based on my training and experience, I understand "kool+kake" to have meant that he obtained the credit card account data first-hand by hacking into customer databases of companies doing business on the Internet.

e. "kool+kake" explained his pricing as follows: "[P]rices can be negotiated, especially for bulk purchases, but as for now, all CVVs, no matter what where or what type of card, will be 7.50\$ each."

f. "kool+kake" ended his posting by instructing interested users to "PM me and I'll send you my MSN." Based on my training and experience, by this remark, I understand "kool+kake" to have meant that interested users should send him a private message through the UC Site, and he would reply with his username on MSN Instant Messenger, a popular instant-messaging, or "chat," service on the Internet, through which they could communicate further.

9. In the days following his December 19, 2010 posting, "kool+kake" received private messages from several users of the UC Site expressing interest in his CVVs. "kool+kake" replied to these users with his MSN Instant Messenger username.

10. On or about January 8, 2011, "kool+kake" started a new discussion thread titled "some free AU CCNs." From reviewing this posting, I know the following:

a. "kool+kake" stated that he was "[l]ooking to trade 14,000 x 100% live AU ccns for some AU cvv, also selling these for 50 cents each." Based on my training and experience, I understand "kool+kake" to have meant that he had 14,000 live Australian credit card numbers that he

wanted either to trade for Australian CVVs - which include a fuller set of credit card data than just the card number - or to sell for 50 cents apiece.

b. "kool+kake" provided several samples of the credit card numbers he had available, along with the expiration date and account holder name corresponding to each number. I have confirmed with representatives of Visa that the credit card numbers correspond to genuine credit card accounts.

11. On or about January 7, 2011, "kool+kake" started a discussion thread titled in part, "PayPal Accounts, Email:Pass Dumps." From reviewing this posting, I know the following:

a. "kool+kake" stated that he had "a nice sized hacked PayPal list that I update daily" and that he would be "selling raw lists of fresh checked PPs." Based on my training and experience, I understand "kool+kake" to have meant that he was selling stolen login information, i.e., usernames and passwords, for user accounts at PayPal, a popular online payment processor. Such login information is used by carders to mine customer accounts for credit card data and personal identification information that can be used in turn to effect fraudulent transactions.

b. As to his pricing, "kool+kake" stated that he would be providing "different bulk options," including \$10 for "4 unique Verified checked PayPals," \$20 for "10 unique Verified checked PayPals," and \$30 for "20 unique Verified checked Paypals."

c. "kool+kake" explained his method of obtaining PayPal login information as follows: "People ask me how I get my Paypals. . . . I do everything manually, including dumping these lists, fresh, from websites, daily So, that said, these are superior quality. I replace instantly, no questions asked, if the account is limited or email/pass is incorrect." Based on my training and experience, I know that carders use the term "dumping" to refer to hacking into and stealing data from databases of personal identification information. Thus, in saying that he "dump[ed]" his "PayPals" "fresh" from "websites," I understand "kool+kake" to have meant that he obtained PayPal accounts by hacking into customer or transaction databases associated with vulnerable websites, and that the accounts he was selling were recently acquired and guaranteed to be active.

d. "kool+kake" also advertised in this posting that he was selling "Email / Pass lists." Based on my training and experience, I understand "kool+kake" to have been referring to lists of e-mail addresses used as usernames for accessing various websites, along with passwords associated with those usernames. Such lists can be used by carders for, among other things, hacking into e-mail accounts and mining the accounts for financial or personal identification information, or sending "phishing" e-mails to large numbers of computer users designed to induce them into replying with financial or personal identification information.

e. "kool+kake" elaborated concerning his "e-mail/pass lists": "The quality of these are very, very good. I've dumped these personally from a very popular online medical learning center, which has well above 100k registrants. I've checked these lists . . . this quality is hard to match." Based on my training and experience, I understand "kool+kake" to have meant that he had obtained the e-mail usernames and passwords he was selling by hacking into a database associated with a popular online medical website, containing registration information for over 100,000 users.

12. Following his initial posting to the January 7, 2011 thread, "kool+kake" repeatedly posted to this thread on occasion thereafter to report that he had freshly acquired login information in stock. For example:

a. On or about February 22, 2011, "kool+kake" posted a message stating that he "[f]inally got Paypals again."

b. On or about March 9, 2011, "kool+kake" posted a message stating: "Back in stock, dumped a nice 100k email/pass list, real superb quality."

c. On or about March 17, 2011, "kool+kake" posted a message stating that he had PayPal accounts "[s]till in stock."

d. On or about March 30, 2011, "kool+kake" posted a message stating that he had one "PP [PayPal] account" for sale with a \$1,000 balance on the account. The message also included three free samples of the PayPal accounts he had for sale, including such information as username, password, account balance, and last log-in.

e. On or about April 6, 2011, "kool+kake" posted a message saying that he had "worldwide PPs" with "balances" "in stock now." The message also included six free samples of the

PayPal accounts he had for sale, including such information as username, password, account balance, and last log-in.

13. On or about March 25, 2011, "kool+kake" started a discussion thread titled "500k+ email::pass dumps." In this posting, "kool+kake" advertised that he was giving away "about 500k+ email/passess" - that is, approximately 500,000 e-mail address/password combinations - for free. "kool+kake" explained, "the reason i'm doing this is because i'm going to start dumping again fresh so figured might as well release my previous material." The posting contained a link to a page on a file-sharing website.

14. I have followed the link provided in the March 25, 2011 posting, which leads to a collection of fifteen files, containing, in total, more than 150,000 unique e-mail username/password combinations. Based on my training and experience, some of the files appear to be reports generated through an automated software tool used to identify websites containing certain types of vulnerabilities. These vulnerabilities can be exploited through so-called "SQL injections" - a method commonly used by computer hackers to obtain unauthorized access into customer databases through company websites. I have confirmed with representatives of websites listed in two of the files that the e-mail addresses listed in the files correspond to registered users of the websites.

15. On or about June 30, 2011, "kool+kake" started a discussion thread titled "Mail+pass / Paypals." In his posting, "kool+kake" stated that he had "extremely fresh dumps" of PayPal accounts and e-mail username/password combinations available. "kool+kake" stated that he was offering them for "\$7 per 1,000," or even lower for larger "bulk orders." As to the types of accounts that the e-mail username/password combinations could be used to access, "kool+kake" stated: "I can sell Ebay - Apple - Amazon - Skype - Zappos - Walmart - Sony - Newegg - Dell accounts and much more."

16. On or about July 10, 2011, "kool+kake" posted a message to his June 30, 2011 thread, again advertising that he had e-mail username/password combinations for sale, this time categorized by e-mail provider, including America Online, Gmail, Yahoo, and Hotmail accounts.

Identification of "kool+kake"

17. On or about June 12, 2011, "kool+kake" exchanged private messages with another UC Site user ("User-1") concerning a fake state identification that "kool+kake" was interested in acquiring. In the exchange, "kool+kake" told User-1 that he wanted to buy a "state id" for "Georgia, USA," adding, "Any address or other information can be made up."

18. I have reviewed logs of the IP addresses used by "kool+kake" to access the UC Site. Many of these IP addresses trace back to AT&T Internet Services, an Internet service provider.

19. I have reviewed records subpoenaed from AT&T Internet Services concerning a sample of the AT&T Internet Services IP addresses used by "kool+kake" to access the UC Site (the "Sample IP Addresses"). According to these records, at the times when the Sample IP Addresses were used by "kool+kake" to access the UC Site, the IP addresses were assigned to a female subscriber of AT&T Internet Services with the last name "Hatala," with an address in Saint Simmons Island, Georgia. Based on a search of law enforcement and publicly available databases, I have learned that this subscriber is a relative who appears to be the grandmother of an individual named "Alex Hatala," who is also a resident of Georgia.

20. Based on a search of the Facebook website, I found a Facebook user named "Alex Hatala" whose Facebook page lists a military academy in Georgia as his high school (the "Alex Hatala Facebook Account").⁶

21. I have subpoenaed records from Facebook concerning the Alex Hatala Facebook Account, which include logs of the IP addresses from which the user of the Alex Hatala Facebook Account logged into the account.

22. From comparing the IP addresses used to access the Alex Hatala Facebook Account with the IP addresses used by "kool+kake" to access the UC Site, and from comparing these records further with the Sample IP Addresses traced to the residence of the individual believed to be Hatala's grandmother, I have learned the following:

⁶ Based on information obtained from law enforcement and publicly available databases, I have determined that the defendant is not a minor, as he was born in January 1993.

a. On July 23, 2011, at approximately 4:32 a.m. GMT, the user of the Alex Hatala Facebook Account logged into the account from the IP address 98.86.140.78.

b. On July 23, 2011, at approximately 4:58 a.m. GMT, "kool+kake" used this same IP address to post a message on the UC Site.

c. This IP address was assigned at both of these times to the residence of the individual believed to be Hatala's grandmother - implying, based on my training and experience, that someone inside the residence accessed both the Alex Hatala Facebook Page and the "kool+kake" account on the UC Site within an approximately 30-minute time frame.

d. On August 11, 2011, at approximately 8:30 a.m. GMT, the user of the Alex Hatala Facebook Account logged into the account using the IP address 98.86.214.194.

e. On August 11, 2011, at approximately 8:42 a.m. GMT, "kool+kake" used this same IP address to post a message on the UC Site.

f. This IP address was assigned at both of these times to the residence of the individual believed to be Hatala's grandmother - implying, based on my training and experience, that someone inside the residence accessed both the Alex Hatala Facebook Account and the "kool+kake" account on the UC Site within an approximately 15-minute time frame.

23. The Facebook records for the Alex Hatala Facebook Page also include subscriber information for the user of the account, which list the user's (self-reported) email address as "dborarnack@yahoo.com."

24. On or about June 18, 2011, "kool+kake" posted a message to a discussion thread on the UC Site concerning "League of Legends," an online video game. In this posting, "kool+kake" mentioned that he played League of Legends under the name "MasterChiefBudz."

25. Based on a Google search of the term "MasterChiefBudz," I located an online discussion forum at <http://forum.grasscity.com>, in which, on or about August 11, 2011, a forum user going by the name "Arnack" posted a message stating that he played League of Legends under the name "MasterChiefBudz."

26. Based on a Google search of the term "Arnack," I located a website located at <http://mohg.bravehost.com>, from which I know the following:

a. The home page of the website contains a banner with the caption: "MOHG: Massive Online Hacking Game."

b. Underneath the banner, the page states: "Welcome to Project: MOHG! The site now is maintained by Arnack. You can contact him at dborarnack@yahoo.com."

c. The home page includes a link captioned "Who Owns MOHG?"


d. Clicking on the link leads to a page on the website containing information about two individuals described as the "owners of MOHG."

e. This page identifies one of the two "owners" as "Arnack," whose e-mail address is listed as "dborarnack@yahoo.com," and whose "Real Name," the page states, is "Alex."

f. The page further provides a brief biography for "Alex," which claims, among other things, that "[a]t the age of 12, he started web hacking."

27. Accordingly, I believe that the UC Site user described above as "kool+kake" is ALEX HATALA, a/k/a "kool+kake," the defendant.

WHEREFORE, I respectfully request that an arrest warrant be issued for ALEX HATALA, a/k/a "kool+kake," the defendant, and that he be arrested and imprisoned or bailed, as the case may be.


CHRISTOPHER J. COPE
Special Agent
Federal Bureau of Investigation

Sworn to before me this
22 day of June 2012


UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK